

FUNDAMENTALS OF QUANTUM MUTUAL ENTROPY AND CAPACITY

Masanori Ohya

Department of Information Sciences
Science University of Tokyo
Noda City, Chiba 278-8510, Japan

1 Introduction

The study of mutual entropy (information) and capacity in classical system was extensively done after Shannon by several authors like Kolmogorov [12] and Gelfand [7]. In quantum systems, there have been several definitions of the mutual entropy for classical input and quantum output [5, 8, 9, 14]. In 1983, the author defined [21] the fully quantum mechanical mutual entropy by means of the relative entropy of Umegaki [35], and he extended it [23] to general quantum systems by the relative entropy of Araki [3] and Uhlmann [34]. When the author introduced the quantum mutual entropy, he did not indicate that it contains other definitions of the mutual entropy including classical one, so that there exist several misunderstandings for the use of the mutual entropy (information) to compute the capacity of quantum channels. Therefore in this note we point out that our quantum mutual entropy generalizes others and where the misuse occurs.

2 Mutual Entropy

The quantum mutual entropy was introduced in [21] for a quantum input and quantum output, namely, for a purely quantum channel, and it was generalized for a general quantum system described by C*-algebraic terminology [23]. We here review the mutual entropy in usual quantum system described by a Hilbert space.

Let \mathcal{H} be a Hilbert space for an input space, $\mathbf{B}(\mathcal{H})$ be the set of all bounded linear operators on \mathcal{H} and $\mathcal{S}(\mathcal{H})$ be the set of all density operators on \mathcal{H} . An output space is described by another Hilbert space $\tilde{\mathcal{H}}$, but often

$\mathcal{H} = \tilde{\mathcal{H}}$. A channel from the input system to the output system is a mapping Λ^* from $\mathcal{S}(\mathcal{H})$ to $\mathcal{S}(\tilde{\mathcal{H}})$ [20]. A channel Λ^* is said to be completely positive if the dual map Λ satisfies the following condition: $\sum_{k,j=1}^n A_k^* \Lambda(B_k^* B_j) A_j \geq 0$ for any $n \in \mathbf{N}$ and any $A_j \in B(\mathcal{H}), B_j \in B(\tilde{\mathcal{H}})$. This condition is not strong at all because almost all physical transformations satisfy it [10, 23].

An input state $\rho \in \mathcal{S}(\mathcal{H})$ is sent to the output system through a channel Λ^* , so that the output state is written as $\tilde{\rho} \equiv \Lambda^* \rho$. Then it is important to ask how much information of ρ is correctly sent to the output state $\Lambda^* \rho$. This amount of information transmitted from input to output is expressed by the mutual entropy.

In order to define the mutual entropy, we first mention the entropy of a quantum state introduced by von Neumann [19]. For a state ρ , there exists a unique spectral decomposition

$$\rho = \sum_k \lambda_k P_k, \quad (2.1)$$

where λ_k is an eigenvalue of ρ and P_k is the associated projection for each λ_k . The projection P_k is not one-dimensional when λ_k is degenerated, so that the spectral decomposition can be further decomposed into one-dimensional projections. Such a decomposition is called a Schatten decomposition [33], namely,

$$\rho = \sum_k \lambda_k E_k, \quad (2.2)$$

where E_k is the one-dimensional projection associated with λ_k and the degenerated eigenvalue λ_k repeats $\dim P_k$ times; for instance, if the eigenvalue λ_1 has the degeneracy 3, then $\lambda_1 = \lambda_2 = \lambda_3 < \lambda_4$. This Schatten decomposition is not unique unless every eigenvalue is non-degenerated. Then the entropy (von Neumann entropy) $S(\rho)$ of a state ρ is defined by

$$S(\rho) = -\text{tr} \rho \log \rho, \quad (2.3)$$

which equals to the Shannon entropy of the probability distribution $\{\lambda_k\}$:

$$S(\rho) = - \sum_k \lambda_k \log \lambda_k. \quad (2.4)$$

The quantum mutual entropy was introduced on the basis of the above von Neumann entropy for purely quantum communication processes. The

mutual entropy depends on an input state ρ and a channel Λ^* , so it is denoted by $I(\rho; \Lambda^*)$, which should satisfy the following conditions:

(1) The quantum mutual entropy is well-matched to the von Neumann entropy. Furthermore, if a channel is trivial, i.e., $\Lambda^* = \text{identity map}$, then the mutual entropy equals to the von Neumann entropy: $I(\rho; id) = S(\rho)$.

(2) When the system is classical, the quantum mutual entropy reduces to classical one.

(3) Shannon's fundamental inequality [32] $0 \leq I(\rho; \Lambda^*) \leq S(\rho)$ is held.

Before mentioning the quantum mutual entropy, we briefly review the classical mutual entropy [6]. Let (Ω, \mathcal{F}) , $(\bar{\Omega}, \bar{\mathcal{F}})$ be an input and output measurable spaces, respectively, and $P(\Omega)$, $P(\bar{\Omega})$ are the corresponding sets of all probability measures (states) on Ω and $\bar{\Omega}$, respectively. A channel Λ^* is a mapping from $P(\Omega)$ to $P(\bar{\Omega})$ and its dual Λ is a map from the set $B(\Omega)$ of all Baire measurable functions on Ω to $B(\bar{\Omega})$. For an input state $\mu \in P(\Omega)$, the output state $\bar{\mu} = \Lambda^* \mu$ and the joint state (probability measure) Φ is given by

$$\Phi(Q \times \bar{Q}) = \int_{\bar{Q}} \Lambda(1_Q) d\mu, \quad Q \in \mathcal{F}, \quad \bar{Q} \in \bar{\mathcal{F}}, \quad (2.5)$$

where 1_Q is the characteristic function on Ω : $1_Q(\omega) = \begin{cases} 1 & (\omega \in Q) \\ 0 & (\omega \notin Q) \end{cases}$. The classical entropy, relative entropy and mutual entropy are defined as follows:

$$S(\mu) = \sup \left\{ - \sum_{k=1}^n \mu(A_k) \log \mu(A_k); \{A_k\} \in \mathcal{P}(\Omega) \right\}, \quad (2.6)$$

$$S(\mu, \nu) = \sup \left\{ \sum_{k=1}^n \mu(A_k) \log \frac{\mu(A_k)}{\nu(A_k)}; \{A_k\} \in \mathcal{P}(\Omega) \right\}, \quad (2.7)$$

$$I(\mu; \Lambda^*) = S(\Phi, \mu \otimes \Lambda^* \mu), \quad (2.8)$$

where $\mathcal{P}(\Omega)$ is the set of all finite partitions on Ω , that is, $\{A_k\} \in \mathcal{P}(\Omega)$ iff $A_k \in \mathcal{F}$ with $A_k \cap A_j = \emptyset$ ($k \neq j$) and $\cup_{k=1}^n A_k = \Omega$.

The quantum mutual entropy is defined as follows: In order to define the quantum mutual entropy, we need the quantum relative entropy and the joint state (it is called "compound state" in the sequel) describing the correlation between an input state ρ and the output state $\Lambda^* \rho$ through a channel Λ^* .

A finite partition of Ω in classical case corresponds to an orthogonal decomposition $\{E_k\}$ of the identity operator I of \mathcal{H} in quantum case because the set of all orthogonal projections is considered to make an event system in a quantum system. It is known [28] that the following equality holds

$$\sup \left\{ - \sum_k \text{tr} \rho E_k \log \text{tr} \rho E_k; \{E_k\} \right\} = -\text{tr} \rho \log \rho,$$

and the supremum is attained when $\{E_k\}$ is a Schatten decomposition of ρ . Therefore the Schatten decomposition is used to define the compound state and the quantum mutual entropy.

The compound state σ_E (corresponding to joint state in CS) of ρ and $\Lambda^* \rho$ was introduced in [21, 22], which is given by

$$\sigma_E = \sum_k \lambda_k E_k \otimes \Lambda^* E_k, \quad (2.9)$$

where E stands for a Schatten decomposition $\{E_k\}$ of ρ , so that the compound state depends on how we decompose the state ρ into basic states (elementary events), in other words, how to see the input state.

The relative entropy for two states ρ and σ is defined by Umegaki [35] and Lindblad [15], which is written as

$$S(\rho, \sigma) = \begin{cases} \text{tr} \rho (\log \rho - \log \sigma) & (\text{when } \overline{\text{ran} \rho} \subset \overline{\text{ran} \sigma}) \\ \infty & (\text{otherwise}) \end{cases} \quad (2.10)$$

Then we can define the mutual entropy by means of the compound state and the relative entropy [21], that is,

$$I(\rho; \Lambda^*) = \sup \{ S(\sigma_E, \rho \otimes \Lambda^* \rho); E = \{E_k\} \}, \quad (2.11)$$

where the supremum is taken over all Schatten decompositions because this decomposition is not unique generally. Some computations reduce it to the following form:

$$I(\rho; \Lambda^*) = \sup \left\{ \sum_k \lambda_k S(\Lambda^* E_k, \Lambda^* \rho); E = \{E_k\} \right\}. \quad (2.12)$$

This mutual entropy satisfies all conditions (1)~(3) mentioned above.

When the input system is classical, an input state ρ is given by a probability distribution or a probability measure, in either case, the Schatten decomposition of ρ is unique, namely, for the case of probability distribution ; $\rho = \{\lambda_k\}$,

$$\rho = \sum_k \lambda_k \delta_k, \quad (2.13)$$

where δ_k is the delta measure, that is,

$$\delta_k(j) = \delta_{k,j} = \begin{cases} 1 & (k=j) \\ 0 & (k \neq j) \end{cases}, \forall j. \quad (2.14)$$

Therefore for any channel Λ^* , the mutual entropy becomes

$$I(\rho; \Lambda^*) = \sum_k \lambda_k S(\Lambda^* \delta_k, \Lambda^* \rho), \quad (2.15)$$

which equals to the following usual expression of Shannon when the minus is well-defined:

$$I(\rho; \Lambda^*) = S(\Lambda^* \rho) - \sum_k \lambda_k S(\Lambda^* \delta_k). \quad (2.16)$$

The above equality has been taken as the definition of the mutual entropy for a classical-quantum channel [4, 5, 8, 9, 14].

Note that the definition (2.12) of the mutual entropy is written as

$$I(\rho; \Lambda^*) = \sup \left\{ \sum_k \lambda_k S(\Lambda^* \rho_k, \Lambda^* \rho); \rho = \sum_k \lambda_k \rho_k \in F_o(\rho) \right\},$$

where $F_o(\rho)$ is the set of all orthogonal finite decompositions of ρ . Here ρ_k is orthogonal to ρ_j (denoted by $\rho_k \perp \rho_j$) means that the range of ρ_k is orthogonal to that of ρ_j . The equality is easily proved as follows: Put

$$I_f(\rho; \Lambda^*) = \sup \left\{ \sum_k \lambda_k S(\Lambda^* \rho_k, \Lambda^* \rho); \rho = \sum_k \lambda_k \rho_k \in F_o(\rho) \right\}.$$

The inequality $I(\rho; \Lambda^*) \leq I_f(\rho; \Lambda^*)$ is obvious. Let us prove the converse. Each ρ_k in an orthogonal decomposition of ρ is further decomposed into one dimensional projections; $\rho_k = \sum_j \mu_j^{(k)} E_j^{(k)}$, a Schatten decomposition of ρ_k . From the following equalities of the relative entropy [3, 28]: (1)

$S(a\rho, b\sigma) = aS(\rho, \sigma) - a \log \frac{b}{a}$, for any positive number a, b ; (2) $\rho_1 \perp \rho_2 \implies S(\rho_1 + \rho_2, \sigma) = S(\rho_1, \sigma) + S(\rho_2, \sigma)$, we have

$$\begin{aligned} \sum_k \lambda_k S(\Lambda^* \rho_k, \Lambda^* \rho) &= \sum_{k,j} \lambda_k \mu_j^{(k)} S(\Lambda^* E_j^{(k)}, \Lambda^* \rho) + \sum_{k,j} \lambda_k \mu_j^{(k)} \log \mu_j^{(k)} \\ &\leq \sum_{k,j} \lambda_k \mu_j^{(k)} S(\Lambda^* E_j^{(k)}, \Lambda^* \rho), \end{aligned}$$

which implies the converse inequality $I(\rho; \Lambda^*) \geq I_f(\rho; \Lambda^*)$ because

$\sum_{k,j} \lambda_k \mu_j^{(k)} E_j^{(k)}$ is a Schatten decomposition of ρ . Thus $I(\rho; \Lambda^*) = I_f(\rho; \Lambda^*)$.

More general formulation of the mutual entropy for general quantum systems was done [23, 10] in C*-dynamical system by using Araki's or Uhlmann's relative entropy [3, 34, 28]. This general mutual entropy contains all other cases including measure theoretic definition of Gelfand and Yaglom [7].

The mutual entropy is a measure for not only information transmission but also description of state change, so that this quantity can be applied to several topics [1, 2, 16, 18, 23, 24, 27, 31].

3 Communication Processes

We discuss communication processes in this section [6, 9, 28]. Let $A = \{a_1, a_2, \dots, a_n\}$ be a set of certain alphabets and Ω be the infinite direct product of A : $\Omega = A^{\mathbb{Z}} \equiv \prod_{-\infty}^{\infty} A$ calling a message space. In order to send a information written by an element of this message space to a receiver, we often need to transfer the message into a proper form for a communication channel. This change of a message is called a coding. Precisely, a coding is a measurable one to one map ξ from Ω to a proper space X . For instance, we have the following codings: (1) When a message is expressed by binary symbol 0 and 1, such a coding is a map from Ω to $\{0, 1\}^{\mathbb{N}}$. (2) A message expressed by 0,1 sequence in (1) is represented by an electric signal. (3) Instead of an electric signal, we use optical signal. Coding is a combination of several maps like the above (1) and (2), (3). One of main targets of the coding theory is to find the most efficient coding and also decoding for information transmission.

Let $(\Omega, \mathcal{F}_\Omega, P(\Omega))$ be an input probability space and X be the coded input space. This space X may be a classical object or a quantum object. For instance, X is a Hilbert space \mathcal{H} of a quantum system, then the coded input system is described by $(B(\mathcal{H}), \mathcal{S}(\mathcal{H}))$ of Sec.2.

An output system is similarly described as the input system: The coded output space is denoted by \tilde{X} and the decoded output space is $\tilde{\Omega}$ made by

another alphabets. An transmission (map) from X to \tilde{X} is described by a channel reflecting all properties of a physical device, which is denoted by γ here. With a decoding $\tilde{\xi}$, the whole information transmission process is written as

$$\Omega \xrightarrow{\xi} X \xrightarrow{\gamma} \tilde{X} \xrightarrow{\tilde{\xi}} \tilde{\Omega}. \quad (3.1)$$

That is, a message $\omega \in \Omega$ is coded to $\xi(\omega)$ and it is sent to the output system through a channel γ , then the output coded message becomes $\gamma \circ \xi(\omega)$ and it is decoded to $\tilde{\xi} \circ \gamma \circ \xi(\omega)$ at a receiver.

This transmission process is mathematically set as follows: M messages are sent to a receiver and the k th message $\omega^{(k)}$ occurs with the probability λ_k . Then the occurrence probability of each message in the sequence $(\omega^{(1)}, \omega^{(2)}, \dots, \omega^{(M)})$ of M messages is denoted by $\rho = \{\lambda_k\}$, which is a state in a classical system. If ξ is a classical coding, then $\xi(\omega)$ is a classical object such as an electric pulse. If ξ is a quantum coding, then $\xi(\omega)$ is a quantum object (state) such as a coherent state. Here we consider such a quantum coding, that is, $\xi(\omega^{(k)})$ is a quantum state, and we denote $\xi(\omega^{(k)})$ by σ_k . Thus the coded state for the sequence $(\omega^{(1)}, \omega^{(2)}, \dots, \omega^{(M)})$ is written as

$$\sigma = \sum_k \lambda_k \sigma_k. \quad (3.2)$$

This state is transmitted through a channel γ . This channel is expressed by a completely positive mapping Γ^* , in the sense of Sec.1, from the state space of X to that of \tilde{X} , hence the output coded quantum state $\tilde{\sigma}$ is $\Gamma^* \sigma$. Since the information transmission process can be understood as a process of state (probability) change, when Ω and $\tilde{\Omega}$ are classical and X and \tilde{X} are quantum, the process (3.1) is written as

$$P(\Omega) \xrightarrow{\Xi^*} \mathcal{S}(\mathcal{H}) \xrightarrow{\Gamma^*} \mathcal{S}(\tilde{\mathcal{H}}) \xrightarrow{\tilde{\Xi}^*} P(\tilde{\Omega}), \quad (3.3)$$

where Ξ^* (resp. $\tilde{\Xi}^*$) is the channel corresponding to the coding ξ (resp. $\tilde{\xi}$) and $\mathcal{S}(\mathcal{H})$ (resp. $\mathcal{S}(\tilde{\mathcal{H}})$) is the set of all density operators (states) on \mathcal{H} (resp. $\tilde{\mathcal{H}}$).

We have to be care to study the objects in the above transmission process (3.1) or (3.3). Namely, we have to make clear which object is going to study. For instance, if we want to know the information capacity of a quantum

channel $\gamma(= \Gamma^*)$, then we have to take X so as to describe a quantum system like a Hilbert space and we need to start the study from a quantum state in quantum space X not from a classical state associated to a message. If we like to know the capacity of the whole process including a coding and a decoding, which means the capacity of a channel $\tilde{\xi} \circ \gamma \circ \xi (= \tilde{\Xi}^* \circ \Gamma^* \circ \Xi^*)$, then we have to start from a classical state. In any case, when we concern the capacity of channel, we have only to take the supremum of the mutual entropy $I(\rho; \Lambda^*)$ over a quantum or classical state ρ in a proper set determined by what we like to study with a channel Λ^* . We explain this more precisely in the next section.

4 Channel Capacity

We discuss two types of channel capacity in communication processes, namely, the capacity of a quantum channel Γ^* and that of a classical (classical-quantum-classical) channel $\tilde{\Xi}^* \circ \Gamma^* \circ \Xi^*$.

(1) *Capacity of quantum channel:* The capacity of a quantum channel is the ability of information transmission of the channel itself, so that it does not depend on how to code a message being treated as a classical object and we have to start from an arbitrary quantum state and find the supremum of the mutual entropy. One often makes a mistake in this point. For example, one starts from the coding of a message and compute the supremum of the mutual entropy and he says that the supremum is the capacity of a quantum channel, which is not correct. Even when his coding is a quantum coding and he sends the coded message to a receiver through a quantum channel, if he starts from a classical state, then his capacity is not the capacity of the quantum channel itself. In his case, usual Shannon's theory is applied because he can easily compute the conditional distribution by a usual (classical) way. His supremum is the capacity of a classical-quantum-classical channel, and it is in the second category discussed below.

The capacity of a quantum channel Γ^* is defined as follows: Let $\mathcal{S}_0(\subset \mathcal{S}(\mathcal{H}))$ be the set of all states prepared for expression of information. Then the capacity of the channel Γ^* with respect to \mathcal{S}_0 is defined by

$$C^{\mathcal{S}_0}(\Gamma^*) = \sup\{I(\rho; \Gamma^*); \rho \in \mathcal{S}_0\}. \quad (4.1)$$

Here $I(\rho; \Gamma^*)$ is the mutual entropy given in (2.11) or (2.12) with $\Lambda^* = \Gamma^*$.

When $\mathcal{S}_0 = \mathcal{S}(\mathcal{H})$, $C^{\mathcal{S}(\mathcal{H})}(\Gamma^*)$ is denoted by $C(\Gamma^*)$ for simplicity. In [29, 17], we also considered the pseudo-quantum capacity $C_p(\Gamma^*)$ defined by (4.1) with the pseudo-mutual entropy $I_p(\rho; \Gamma^*)$ where the supremum is taken over all finite decompositions instead of all orthogonal pure decompositions:

$$I_p(\rho; \Gamma^*) = \sup \left\{ \sum_k \lambda_k S(\Gamma^* \rho_k, \Gamma^* \rho); \rho = \sum_k \lambda_k \rho_k, \text{ finite decomposition} \right\}. \quad (4.2)$$

However the pseudo-mutual entropy is not well-matched to the conditions explained in Sec.2, and it is difficult to be computed numerically [30]. From the monotonicity of the mutual entropy [28], we have

$$0 \leq C^{\mathcal{S}_0}(\Gamma^*) \leq C_p^{\mathcal{S}_0}(\Gamma^*) \leq \sup \{S(\rho); \rho \in \mathcal{S}_0\}.$$

(2) *Capacity of classical-quantum-classical channel:* The capacity of C-Q-C channel $\tilde{\Xi}^* \circ \Gamma^* \circ \Xi^*$ is the capacity of the information transmission process starting from the coding of messages, therefore it can be considered as the capacity including a coding (and a decoding). As is discussed in Sec.3, an input state ρ is the probability distribution $\{\lambda_k\}$ of messages, and its Schatten decomposition is unique as (2.13), so the mutual entropy is written by (2.15):

$$I(\rho; \tilde{\Xi}^* \circ \Gamma^* \circ \Xi^*) = \sum_k \lambda_k S(\tilde{\Xi}^* \circ \Gamma^* \circ \Xi^* \delta_k, \tilde{\Xi}^* \circ \Gamma^* \circ \Xi^* \rho). \quad (4.3)$$

If the coding Ξ^* is a quantum coding, then $\Xi^* \delta_k$ is expressed by a quantum state. Let denote the coded quantum state by σ_k and put $\sigma = \Xi^* \rho = \sum_k \lambda_k \sigma_k$. Then the above mutual entropy is written as

$$I(\rho; \tilde{\Xi}^* \circ \Gamma^* \circ \Xi^*) = \sum_k \lambda_k S(\tilde{\Xi}^* \circ \Gamma^* \sigma_k, \tilde{\Xi}^* \circ \Gamma^* \sigma). \quad (4.4)$$

This is the expression of the mutual entropy of the whole information transmission process starting from a coding of classical messages. Hence the capacity of C-Q-C channel is

$$C^{P_0}(\tilde{\Xi}^* \circ \Gamma^* \circ \Xi^*) = \sup \{I(\rho; \tilde{\Xi}^* \circ \Gamma^* \circ \Xi^*); \rho \in P_0\}, \quad (4.5)$$

where $P_0(\subset P(\Omega))$ is the set of all probability distributions prepared for input (a-priori) states (distributions or probability measures). Moreover the

capacity for coding is found by taking the supremum of the mutual entropy (4.4) over all probability distributions and all codings Ξ^* :

$$C_c^{P_0}(\tilde{\Xi}^* \circ \Gamma^*) = \sup\{I(\rho; \tilde{\Xi}^* \circ \Gamma^* \circ \Xi^*); \rho \in P_0, \Xi^*\}. \quad (4.6)$$

The last capacity is for both coding and decoding and it is given by

$$C_{cd}^{P_0}(\Gamma^*) = \sup\{I(\rho; \tilde{\Xi}^* \circ \Gamma^* \circ \Xi^*); \rho \in P_0, \Xi^*, \tilde{\Xi}^*\}. \quad (4.7)$$

These capacities $C_c^{P_0}$, $C_{cd}^{P_0}$ do not measure the ability of the quantum channel Γ^* itself, but measure the ability of Γ^* through the coding and decoding.

Remark that $\sum_k \lambda_k S(\Gamma^* \sigma_k)$ is finite, then (4.4) becomes

$$I(\rho; \tilde{\Xi}^* \circ \Gamma^* \circ \Xi^*) = S(\tilde{\Xi}^* \circ \Gamma^* \sigma) - \sum_k \lambda_k S(\tilde{\Xi}^* \circ \Gamma^* \sigma_k). \quad (4.8)$$

Further, if ρ is a probability measure having a density function $f(\lambda)$ and each λ corresponds to a quantum coded state $\sigma(\lambda)$, then $\sigma = \int f(\lambda) \sigma(\lambda) d\lambda$ and

$$I(\rho; \tilde{\Xi}^* \circ \Gamma^* \circ \Xi^*) = S(\tilde{\Xi}^* \circ \Gamma^* \sigma) - \int f(\lambda) S(\tilde{\Xi}^* \circ \Gamma^* \sigma(\lambda)) d\lambda, \quad (4.9)$$

which is less than

$$S(\Gamma^* \sigma) - \int f(\lambda) S(\Gamma^* \sigma(\lambda)) d\lambda.$$

The above bound is called Holevo bound, and it is computed in several cases[29, 36].

The above three capacities C^{P_0} , $C_c^{P_0}$, $C_{cd}^{P_0}$ satisfy the following inequalities

$$0 \leq C^{P_0}(\tilde{\Xi}^* \circ \Gamma^* \circ \Xi^*) \leq C_c^{P_0}(\tilde{\Xi}^* \circ \Gamma^*) \leq C_{cd}^{P_0}(\Gamma^*) \leq \sup\{S(\rho); \rho \in P_0\}$$

where $S(\rho)$ is not the von Neumann entropy but the Shannon entropy: $-\sum \lambda_k \log \lambda_k$.

The capacities (4.1), (4.6), (4.7) and (4.8) are generally different. Some misunderstandings occur due to forgetting which channel is considered. That is, we have to make clear what kind of the ability, the capacity of a quantum channel itself or that of a classical-quantum(-classical) channel or that of a coding free, is considered.

References

- [1] L. Accardi, M. Ohya and H. Suyari, Computation of Mutual Entropy in Quantum Markov Chains, Open Systems and Information Dynamics, **2**, No.3, 337-354, 1994.
- [2] S. Akashi, The asymptotic behavior of ε -entropy of a compact positive operator, J.Math.Anal.Appl., **153**, 250-257, 1990.
- [3] H. Araki, Relative entropy for states of von Neumann algebras, Publ. RIMS Kyoto Univ., **11**, 809-833, 1976.
- [4] V.P. Belavkin, Conditional entropy and capacity of quantum channels, in Proc. of VIII-th Conference on Coding Theory and Information Transmission, 15-19, Moscow-Kuibishev, 1982.
- [5] V.P. Belavkin and P.L. Stratonovich, Optimization of processing of quantum signals according to an information Criterion, Radio Eng. Electron. Phys., **18**, 9, 1839-1844, 1973.
- [6] P. Billingsley, "Ergodic Theory and Information", Wiley, NY., 1965.
- [7] I.M. Gelfand and A.M. Yaglom, Calculation of the amount of information about a random function contained in another such function, Amer. Math. Soc. Transl., **12**, 199-246, 1959.
- [8] A.S. Holevo, Some estimates for the amount of information transmittable by a quantum communication channel (in Russian), Problemy Peredachi Informacii, **9**, 3-11, 1973
- [9] R.S. Ingarden, Quantum information theory, Rep. Math. Phys., **10**, 43-73, 1976.
- [10] R.S. Ingarden, A. Kossakowski and M. Ohya, "Information Dynamics and Open Systems", Kluwer Academic Publishers, 1997.
- [11] K. Inoue, M. Ohya and H. Suyari, Characterization of quantum teleportation processes by nonlinear quantum channel and quantum mutual entropy, to appear in Physica D.
- [12] A.N. Kolmogorov, Theory of transmission of information, Amer. Math. Soc. Translation, Ser.2, **33**, 291-321, 1963.

- [13] S. Kullback and R. Leibler, On information and sufficiency, *Ann. Math. Stat.*, **22**, 79–86, 1951.
- [14] L.B. Levitin, Physical information theory for 30 years: basic concepts and results, *Springer Lect. Note in Phys.*, **378**, 101-110, 1991.
- [15] G. Lindblad, Entropy, information and quantum measurements, *Commun. Math. Phys.*, **33**, 111-119, 1973.
- [16] T. Matsuoka and M. Ohya, Fractal dimensions of states and its application to Ising model, *Rep. Math. Phys.*, **36**, 365–379, 1995.
- [17] N. Muraki, M. Ohya and D. Petz, Note on entropy of general quantum systems, *Open Systems and Information Dynamics*, **1**, **No.1**, 43–56, 1992.
- [18] N. Muraki and M. Ohya, Entropy functionals of Kolmogorov Sinai type and their limit theorems, *Letters in Mathematical Physics*, **36**, 327-375, 1996.
- [19] J.von Neumann, “Die Mathematischen Grundlagen der Quantenmechanik”, Springer-Berlin, 1932.
- [20] M. Ohya, Quantum ergodic channels in operator algebras, *J. Math. Anal. Appl.* **84**, 318-327, 1981.
- [21] M. Ohya, On compound state and mutual information in quantum information theory, *IEEE Trans. Information Theory*, **29**, 770-777, 1983.
- [22] M. Ohya, Note on quantum probability, *L. Nuovo Cimento*, **38**, 402–406, 1983.
- [23] M. Ohya, Some aspects of quantum information theory and their applications to irreversible processes, *Rep. Math. Phys.*, **27**, 19–47, 1989.
- [24] M. Ohya, Fractal dimensions of states, *Quantum Probability and Related Topics*, **6**, World Scientific, Singapore, 1991.
- [25] M. Ohya, State change, complexity and fractal in quantum systems, *Quantum Communications and Measurement*, 309–320, 1995.

- [26] M. Ohya, Complexity and fractal dimensions for quantum states, *Open Systems and Information Dynamics*, **4**, **No.1**, 141-157.
- [27] M. Ohya, Complexities and their applications to characterization of chaos, *International J. Theor. Phys*, **37**, **No.1**, 495-506.
- [28] M. Ohya and D. Petz, “Quantum Entropy and Its Use”, Springer, 1993.
- [29] M. Ohya, D. Petz and N. Watanabe, On capacities of quantum channels, *Probability and Mathematical Statistics*, **17**, 179-196, 1997.
- [30] M. Ohya, D. Petz and N. Watanabe, Numerical computation of quantum capacity, *International J. Theor. Phys.*, **37**, **No.1**, 507-510.
- [31] M. Ohya and N. Watanabe, On mathematical treatment of Fredkin-Toffoli-Milburn gate, to appear in *Physica D*.
- [32] C.E. Shannon, Mathematical theory of communication, *Bell System Tech. J.* **27**, 379–423, 1948.
- [33] R. Schatten, “Norm Ideals of Completely Continuous Operators”, Springer-Verlag, 1970.
- [34] A. Uhlmann, Relative entropy and the Wigner-Yanase-Dyson-Lieb concavity in interpolation theory, *Commun. Math. Phys.*, **54**, 21–32, 1977.
- [35] H. Umegaki, Conditional expectations in an operator algebra IV (entropy and information), *Kodai Math. Sem. Rep.*, **14**, 59–85, 1962.
- [36] H.P. Yuen and M. Ozawa, Ultimate information carrying limit of quantum systems, *Phys. Rev. Lett.*, **70**, 363-366, 1993.